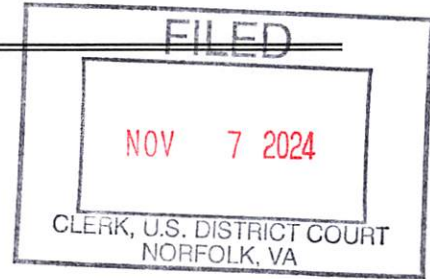


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Android cell phone in a black case, seized on November
1, 2024, outside of Dorsey Rd. in Newport News, VA
and in FBI custody

Case No. 4:24-sw-147

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. § 2252A(a)(1)
 18 U.S.C. § 2252A(a)(2)
 18 U.S.C. § 2252A(a)(5)(B)

Offense Description
 Transportation of Child Pornography
 Receipt of Child Pornography
 Possession of Child Pornography

The application is based on these facts:

See affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

Peter G. Osyf
 Assistant United States Attorney

Applicant's signature

Heather Call, Task Force Officer, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/07/2024City and state: Norfolk, Virginia

Judge's signature

The Honorable Robert J. Krask, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

DESCRIPTION OF THE ITEM TO BE SEARCHED

The item to be searched is described as follows:

The item is an **Android cell phone in a black case** that was seized on November 1, 2024, from Christopher Ingram's vehicle outside of 4 Dorsey Rd, Newport News, Virginia, 23606. It is currently located at the Federal Bureau of Investigation (FBI) Peninsula Resident Agency, located at 11827 Canon Blvd, Suite 300, Newport News, Virginia, 23606. (the "**SUBJECT DEVICE**").

ATTACHMENT B

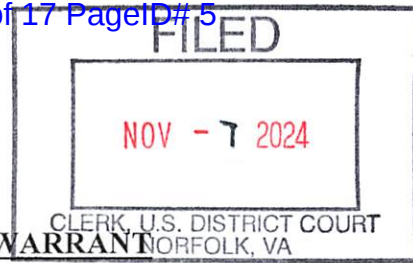
DESCRIPTION OF ITEMS TO BE SEIZED

The items to be seized as evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), include the following:

1. Evidence and records contained within the **SUBJECT DEVICE** to include:
 - a. evidence of who used, owned, or controlled the **SUBJECT DEVICE** (also referred to as “computer” hereafter) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the **SUBJECT DEVICE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the **SUBJECT DEVICE** was accessed or used to determine the chronological context of **SUBJECT DEVICE** access, use, and events relating to the crime(s) under investigation and to the computer user;
 - e. evidence indicating the **SUBJECT DEVICE** user’s knowledge and/or intent as it relates to the crime(s) under investigation;
 - f. evidence of attachment to the **SUBJECT DEVICE** of other storage devices or similar containers for electronic evidence;
 - g. evidence of programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICE**;
 - h. evidence of the times the **SUBJECT DEVICE** was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICE**;
 - j. documentation and manuals that may be necessary to access the **SUBJECT DEVICE** or to conduct a forensic examination of the **SUBJECT DEVICE**;
 - k. records of or information about Internet Protocol addresses used by the

SUBJECT DEVICE;

- l. records of or information about the **SUBJECT DEVICE's** Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. records and information relating to the sexual exploitation of children, including indications of the use of social media and communication platforms, including, but not limited to: Synchronoss, Telegram, Facebook, Kik, Instagram, Snapchat, Dropbox, Whisper, etc.; and
 - n. contextual information necessary to understand the evidence described in this attachment.
2. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.
3. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.



AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

Introduction and Agent Background

I, Heather Call, being duly sworn, hereby depose and state:

1. Your affiant, Heather Call, employed with the Newport News Police Department (NNPD) since June 2004, and more specifically with the Special Victims Unit since July 2011. This assignment has afforded me the opportunity to investigate and/or arrest and prosecute numerous individuals for crimes relating to the neglect and abuse of children in violation of the Virginia (VA) State Code. I have previously been involved in criminal investigations concerning violations of federal laws. Those investigations included, but are not limited to, child exploitation and child pornography. Since joining the NNPD your affiant has attended specialized training courses in child/adolescent interviewing, human trafficking, identifying, and seizing electronic evidence, and computer forensic, recovery, and social site investigations.

2. I am currently assigned as a Master Police Detective with the Newport News Police Department, Criminal Investigations Division, Special Victims Unit, as well as a Task Force Officer (TFO) assigned to the Federal Bureau of Investigation, Norfolk Division Child Exploitation Task Force. I have participated in investigations involving sexual assaults, persons who collect and distribute child pornography, and distribution of materials relating to the sexual exploitation of children. I have received training from the FBI in the areas of sexual assaults and child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers.

3. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18, United States Code § 2251 *et. seq.* involving child exploitation offenses.

4. I was deputized as a Special Deputy United States Marshal on June 16, 2014. As a Special Deputy United States Marshal, your Affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

Location

5. This affidavit is made in support of an application for a warrant to search the item described as an **Android cell phone in a black case** (more precisely described in Attachment A).

6. This affidavit is based upon information that I have gained from my investigation, my training and experience, as well as information gained from conversations with other law

enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities (more precisely described in Attachment B) of violations of Title 18, United States Code, Sections 2252A(a)(1), 2252A(a)(2), and 2252A(a)(5)(B) are located on the above item.

Pertinent Federal Criminal Statutes

7. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252A(a)(1), 2252A(a)(2), and 2252A(a)(5)(B), relating to material involving the sexual exploitation of minors.

8. Title 18, United States Code, Section 2252A(a)(1) makes it a federal criminal offense to knowingly mail, or transport or ship using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography.

9. Title 18, United States Code, Section 2252A(a)(2) makes it a federal criminal offense to knowingly receive or distribute any child pornography or materials that contains child pornography that has been mailed or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

10. Title 18, United States Code, Section 2252A(a)(5)(B) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

Definitions

11. The term “computer,” as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

12. The terms “records,” “documents,” and “materials” include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

Graphic records or representations, photographs, pictures, images, and aural records or representations.

13. The terms “minor” and “sexually explicit conduct” are defined in Title 18, United States Code, Sections 2256(1) and (2). A “minor” is defined as “any person under the age of eighteen years.” The term “sexually explicit conduct” means actual or simulated:

- i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
- ii. Bestiality;
- iii. Masturbation;
- iv. Sadistic or masochistic abuse; or
- v. Lascivious exhibition of the anus, genitals or pubic area of any person.

14. Universal Resource Locator (URL): A URL is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

15. Internet Protocol Address (IP Address): Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. There are two types of IP addresses, static and dynamic. A static address is permanent and never changes, such as ones used in cable modems. The dynamic address changes almost every time the computer connects to the Internet.

16. The term “Internet Service Provider” (ISPs): This term refers to individuals who have an Internet account and an Internet-based electronic mail (e-mail) address, who must have a subscription, membership, or affiliation with an organization or commercial service that provides access to the Internet. A provider of Internet access and services is referred to as an Internet Service Provider or “ISP.”

17. The term “Secure Hash Algorithm” (SHA-1) is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard. SHA-1 is the original 160-bit hash function. It was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. The SHA-1 value is one form of an electronic fingerprint for a digital image.

18. “Web hosts” provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is “shared,” which means that multiple websites of unrelated companies are on the same server in

order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

19. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

20. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." 18 U.S.C. § 2711.

21. "Electronic Communications System" means any wire, radio, electromagnetic, photo-optical, or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

22. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

23. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17).

Specifics of Search and Seizure of Computer System and Related Media

24. Your affiant, based on conversations with Computer Investigative Specialists, who have been trained in the seizure, examination and retrieval of data from personal computer systems and related media, knows that searching and seizing information from computer systems often requires agents to seize all electronic storage devices to be searched later in a laboratory or other controlled environment.

25. Computer storage devices (like hard drives, diskettes, tapes, laser disks, and thumb or flash drives) can store enormous quantities of information. For instance, a single 200-gigabyte hard-drive may contain the electronic equivalent of hundreds of thousands of pages of double-spaced text. However, unlike the search of documentary files, computers store data in files that are often not easily reviewed. Additionally, a suspect may try to conceal criminal evidence by storing files in random order and/or with deceptive file names. This may require the examiner to

examine all the stored data to determine which particular files are evidence or instrumentalities of the crime. This sorting process can take weeks or months, depending on the volume of data stored.

26. Searching computer systems for criminal evidence is a highly technical process, requiring specialized skills and a properly controlled environment. The vast array of computer hardware and software available requires even computer examiners to specialize in some systems and applications, so it is difficult to know before a search which computer investigative specialist is qualified to analyze the system and its data. In any event, the investigative specialist will use certified forensic tools and data search protocols that are designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (from external sources and/or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

27. An important step that is ordinarily part of an examiner's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

Use of Computers with Child Pornography

28. Based upon my training and information officially supplied to me by other law enforcement officers, your affiant knows the following:

29. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. They have also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

30. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution and storage.

- a. Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video

camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as methods that have been used in the past.

- b. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer has also changed that. A device known as a modem allows any computer to connect to another computer using telephone lines or other cable lines. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial concerns, such as Microsoft and America Online, which allow subscribers to access their network services via connection through an Internet broadband provider or by dialing a local number and connecting via a telephone modem.
- c. These service providers allow electronic mail ("e-mail") service between subscribers and between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web; hence, they are commonly described as Internet Service Providers (ISPs). Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time using a mode of communication called instant messaging, or "IM." When logged into an IM service, users can search for other users based on the information that the other users have supplied, and they can send those users messages or initiate a chat session. Chat sessions can occur in multiple person groups, or in private one-on-one sessions. Most IM services also allow files to be transferred between users, including image files.
- d. These communications structures are ideal for the child pornography collector. The open and anonymous communication allows users to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send text messages and graphic images to other trusted child pornography collectors. Moreover, the child pornography collectors can use standard Internet connections, such as those provided by business, universities, and government agencies, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively

secure, and anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornography collectors.

- e. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred (via electronic mail, through file transfer protocols (FTPs), or via news group postings) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, and easy access to the Internet, the computer is a preferred method of distribution of child pornographic materials.

31. The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of five hundred (500) gigabytes are not uncommon. These drives can store hundreds of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

32. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for extended periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

Probable Cause to Search

33. Between December 2022 and February 2023, the National Center for Missing and Exploited Children (NCMEC) received five CyberTip Reports (144937974, 154630510, 154746766, 154951164, and 155498289) from Synchronoss Technologies, Inc. From the five CyberTips, Synchronoss Technologies, Inc. reported the Subject Account phone number of the suspect as: 757-303-1230. NCMEC subsequently passed the CyberTips to Bedford County Sheriff's Office (BCSO), in which BCSO passed to FBI Norfolk. In each of the CyberTips, Synchronoss Technologies, Inc. and NCMEC acknowledged and or/listed the images they viewed.

34. In CyberTip 144937974, Synchronoss Technologies, Inc. reported the suspect uploaded four files containing child pornography on December 30, 2022, at 03:37:21 UTC. The Subject Account phone number of the suspect was reported as: 757-303-1230. Synchronoss Technologies, Inc. advised they viewed the entire contents of the uploaded files. A review of the files are listed below:

- a. "f25373840b174d15b2910ebba625b098_064a174df33b2c7f81f86cb84030b732ff343a917a435b7976ebf9ae457cd9bd.mp4": This video file is approximately 53 seconds in length. It is of a prepubescent female juvenile performing oral sex on an adult male.
- b. "f25373840b174d15b2910ebba625b098_096db00e6345815b2a94fd1d8a850089b0c564724f004af333c331cfa50c8dbd.mp4": This video file is approximately 1 minute 3 seconds in length. It is of a prepubescent female juvenile engaged in sexual intercourse with an adult male.

35. In CyberTip 154630510, Synchronoss Technologies, Inc. reported the suspect uploaded 18 files containing child pornography on February 5, 2023, at 22:07:50 UTC. The Subject Account phone number of the suspect was reported as: 757-303-1230. Synchronoss Technologies, Inc. advised they viewed the entire contents of the uploaded files. A review of a sampling of the files are listed below:

- a. "f25373840b174d15b2910ebba625b098_6b9b6abe5d0b50fd5293b072598b015af3188a9a22d1df297a01df9111082976.mpf": This is a video file approximately 1 minute 46 seconds in length. It is of a nude female toddler. An adult male rubs his erect penis around her buttocks and between her legs. He then attempts to engage in anal sex with her.
- b. "f25373840b174d15b2910ebba625b098_7cb2db49fc1ff2dd2c26c92811059a84f80dca5ee0671343544f1d6aeef15998.mp4": This is a video file approximately 2 minutes 13 seconds in length. It is of a nude prepubescent female juvenile wearing a mask on her face. An adult male, also wearing a mask, shoves his fingers into her vagina. She then performs oral sex on him.

36. In CyberTip 154746766, Synchronoss Technologies, Inc. reported the suspect uploaded 16 files containing child pornography on February 7, 2023, at 23:47:23 UTC. The Subject Account phone number of the suspect was reported as: 757-303-1230. Synchronoss Technologies, Inc. advised they viewed the entire contents of the uploaded files. A review of a sampling of the files are listed below:

- a. "f25373840b174d15b2910ebba625b098_ba5d8d49a54e8c158cd154fa5f248eaf0d1dea13d40e04b51f00dc78bf5c6fd8.mp4": This is a video file approximately 28 seconds in length. It is of a nude female infant sitting on an adult female's lap. The adult female rubs her fingers on the infant's genitals.
- b. "f25373840b174d15b2910ebba625b098_48c372351fe3a2ff5a4f02eced56afcacf907af10aa7fbbea45dca63f0aa263b.mp4": This is a video file approximately 42 seconds in length. It is of a prepubescent female juvenile who performs oral sex on a prepubescent male juvenile.

37. In CyberTip 154951164, Synchronoss Technologies, Inc. reported the suspect uploaded 14 files containing child pornography on February 9, 2023, at 21:50:19 UTC. The Subject Account phone number of the suspect was reported as: 757-303-1230. Synchronoss Technologies, Inc. advised they viewed the entire contents of the uploaded files. A review of a sampling of the files are listed below:

- a. "f25373840b174d15b2910ebba625b098_af4cda929af69e675279a7f844b424361a0c956456ba0979f021939f5376c0e4.mp4": This is video file approximately 1 minute 31 seconds in length. It is of a nude prepubescent female juvenile performing oral sex on an adult male.
- b. "f25373840b174d15b2910ebba625b098_7f290bdce56dff42babecb30d4239591766a935da0fae0a0838406678a8e9a6d.mp4": This is a video file approximately 36 seconds in length. It is of a nude prepubescent female juvenile engaged in sexual intercourse with an adult male.

38. In CyberTip 155498289, Synchronoss Technologies, Inc. reported the suspect uploaded four files containing child pornography on February 18, 2023, at 21:39:59 UTC. The Subject Account phone number of the suspect was reported as: 757-303-1230. Synchronoss Technologies, Inc. advised they viewed the entire contents of the uploaded files. A review of a sampling of the files are listed below:

- a. "f25373840b174d15b2910ebba625b098_eabb3515c8160b4f0e391fa554ebb542bbff793ddf439d5829871dc3c3ec9242.mp4": This is a video file approximately 1 minute 4 seconds in length. It is of a prepubescent female juvenile wearing a mask. She is performing oral sex on an adult male.

- b. "f25373840b174d15b2910ebba625b098_1dbfb2ef2c42092feada87cb39d728c0be744249a793e93b7fe79f96d129a176.mp4: This is a video file approximately 25 seconds in length. It is of an adult female performing oral sex on a prepubescent male juvenile.

39. On April 8, 2024, your affiant served an administrative subpoena on Verizon Wireless for customer information pertaining to the phone number 757-303-1230. Verizon provided the account holder as Keshia D. Slack, 4 Dorsey Rd, Apt A, Newport News, Virginia, 23606.

40. Your affiant checked a law enforcement database and found on November 6, 2018, a person named "Christopher" called Newport News police dispatch from the phone number 757-303-1230 to request a medic for an unknown female with wrist pain.

41. Your affiant checked another law enforcement database and found 757-303-1230 to be affiliated with Christopher Ingram, 4 Dorsey Rd, Apt A, Newport News, Virginia, 23606.

42. Your affiant checked Christopher Ingram through the Google search engine and found a baby registry on The Bump. It showed Keshia Ingram and Christopher Ingram's registry with a due date listed as October 30, 2024, and a location as Newport News, Virginia.

43. On October 21, 2024, at 2:21 p.m., while viewing technical surveillance, a male matching Christopher Ingram's DMV photograph came from the area of the front of 4 Dorsey Rd, Apartment A, Newport News, Virginia, 23608 and entered a vehicle registered to Christopher Ingram and Keshia Ingram.

44. On October 23, 2024, while viewing technical surveillance, a male matching Christopher Ingram's DMV photography was seen several times coming from the area in the front of 4 Dorsey Rd, Apartment A, Newport News, Virginia, 23608 and entering a vehicle registered to Christopher Ingram and Keshia Ingram.

45. According to a post on Facebook, Keshia Ingram gave birth to the Ingram's first child on Friday, October 25, 2024.

46. On October 30, 2024, your affiant obtained two federal search warrants and a criminal complaint from the Honorable United States Magistrate Judge Lawrence R. Leonard. The first search warrant was for the Synchronoss Technologies account associated with the phone number 757-303-1230. The second search warrant was for electronic items of evidence in the residence, located at 4 Dorsey Rd, Apartment A, Newport News, Virginia, 23608. The complaint was for the arrest of Christopher Ingram for Transportation of Child Pornography.

47. On November 1, 2024, Christopher Ingram was arrested in the parking lot outside 4 Dorsey Rd, Newport News, Virginia, as he returned to his residence in his vehicle. His cell phone was seized from his vehicle.

48. On November 1, 2024, Christopher Ingram was advised his *Miranda* rights and agreed to speak with your affiant and Special Agent (SA) Jeffrey Noel. A summary of his interview is as follows:

- a. Ingram confirmed his cell phone number was 757-303-1230.
- b. Ingram initially said his cell phone was always being hacked and explained he had a Facebook page tied to his phone number that he can no longer access. He also stated he had let people use his cell phone when he went downtown, but he tried real hard not to let anyone use it.
- c. Ingram denied looking at child pornography, however he had looked at adult pornography until he stopped this year. Ingram talked about communicating with individuals on Snapchat. He said he paid for and downloaded packets of pornography from these individuals. In those packets he would receive "that stuff", but denied looking for it and said he did not like it. He said it happened so many times, but the child pornography was not what he asked for. Ingram stated he would text the individuals back once he found the child pornography and they would tell him that was what he paid for. Ingram talked about being scammed after he sent money for pornography packets, but never received it. Ingram got rid of it because he did not want to masturbate anymore and wanted to do better with his life.
- d. Ingram denied there was any child pornography on his cell phone. He identified his cell phone as being in his vehicle and provided the passcode for the cell phone. It was found to be an **Android cell phone in a black case.**

Biometric Unlock of Devices Subject to Warrant

~~49. I ask that the search warrant, to the extent it authorizes the seizure and search of the electronic devices, authorize the use of the biometric unlock features on any such devices owned and/or used by the device user based on the following, which I know from my training, experience, and review of publicly available materials.~~

~~50. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.~~

~~51. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device~~

~~may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.~~ *RGK* *HC*

~~52. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the device user's thumb-and/or fingers on the device(s); and (2) hold the device(s) in front of the device user's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.~~ *RGK* *HC*

Conclusion

53. Based on the facts set forth above, your affiant believes probable cause exists that located on the **Android cell phone in a black case**, are violations of Title 18, United States Code, Sections 2252A(a)(1), 2252A(a)(2), and 2252A(a)(5)(B), which prohibits knowing transportation, receipt or distribution of child pornography (and any visual depictions of and involving the use of a minor engaging in sexually explicit conduct) in interstate or foreign commerce, and the knowing possession of one or more matters containing an image of child pornography (and any visual depictions of and involving the use of a minor engaging in sexually explicit conduct) that have traveled in interstate or foreign commerce or were produced using material so transported or shipped.

53. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities (more precisely described in Attachment B) of such violations will be found on the **Android cell phone in a black case** (more precisely described in Attachment A.)

55. Accordingly, your affiant requests that a search warrant be issued authorizing FBI agents, representatives of the FBI, with assistance from representatives of other law enforcement agencies as required, to search **Android cell phone in a black case**, (more precisely described in Attachment A), for evidence, fruits, and instrumentalities (more precisely described in Attachment B) of the offenses described in paragraphs 8-10 of this affidavit.

FURTHER AFFIANT SAYETH NOT.



Heather Call
Special Deputy United States Marshal
FBI Child Exploitation Task Force
Federal Bureau of Investigation


This affidavit has been reviewed for legal sufficiency by Assistant United States Attorney Peter G. Osyf.

Reviewed:



Peter G. Osyf
Assistant United States Attorney

Subscribed and sworn before me this 7th day of November 2024, in the City of Norfolk, Virginia.



The Honorable Robert J. Krask
UNITED STATES MAGISTRATE JUDGE